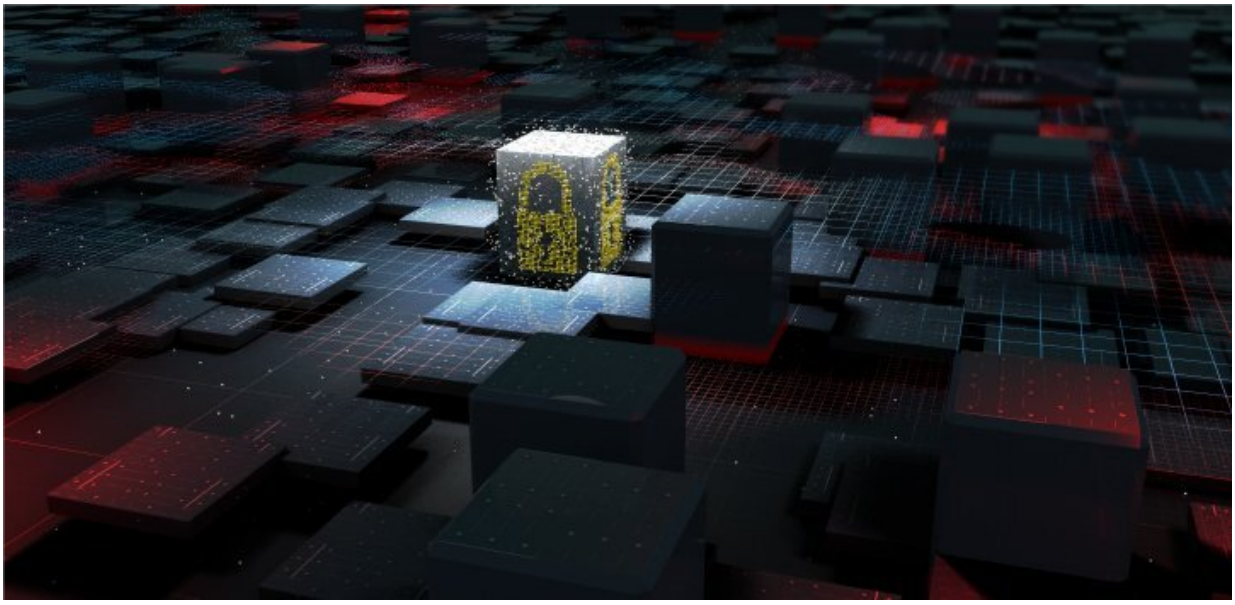
Integrated circuit logic lock based on a magnetic tunnel junction for chip security

November 15 2022



A team of KAUST scientists has designed an integrated circuit logic lock that could represent a leap forward in protecting our electronic devices from cyberattacks. Credit: KAUST; Heno Hwang

Next-generation electronic devices could feature enhanced security systems built directly into their circuitry to help fend off malicious attacks. Protective "logic locks"—based on an advanced branch of electronics called spintronics—could be incorporated into the integrated circuits of electronic chips to defend chip security, KAUST researchers have shown. Their study is published in *IEEE Access*.

"The need for hardware-based security features reflects the globalized nature of modern electronics manufacture," explains Yehia Massoud from KAUST.

Electronics companies usually employ large specialized, external foundries to produce their chips, which minimizes costs but introduces potential vulnerabilities to the supply chain. The circuit design could simply be illegally copied by an untrusted foundry for counterfeit chip production or could be maliciously modified by the incorporation of "hardware Trojans" into the circuitry that detrimentally affects its behavior in some way.

"To increase confidence in the globalized integrated circuit manufacturing chain, security approaches such as logic locking are now widely used," says Divyanshu Divyanshu, a Ph.D. student in Massoud's labs. To defend chip security, the ITL team designed an integrated circuit logic lock based on a component called a magnetic tunnel junction (MTJ).

Logic locking works like a combination lock, Divyanshu explains. Unless the correct "key" combination signal is supplied to the lock, the circuit's operation is scrambled. "The keys to the lock are stored in tamper-proof memory, ensuring hardware security against several threat models," Divyanshu says.

The logic-locking behavior of the MTJ is based on spintronics, an emerging form of advanced electronics. "Spintronics is a field of study in which a physical property of electrons called spin is exploited, in addition to their charge," Massoud explains.

The MTJ's electronic output depends on the spin alignment of the electrons within it. Only when the MTJ receives the correct key signal input, however, does it produce the correct output for the protected

circuit to function.

Spin-based devices have several advantages compared to conventional silicon components, Massoud notes, including low operational voltage and no power consumption during standby.

"With the advancement in fabrication methods, the possibility of using emerging spintronic device structures in the chip design has increased," he adds. "These properties make spintronic devices a potential choice for exploring hardware security."

Spintronics could be ideal for the logic-locking task, the team's work has shown. "Our next steps include the investigation of other spin-based devices to develop logic-locking blocks, with the help of state-of-the-art fabrication facilities available at KAUST," Massoud says.

More information: Divyanshu Divyanshu et al, Logic Locking Using Emerging 2T/3T Magnetic Tunnel Junctions for Hardware Security, *IEEE Access* (2022). DOI: 10.1109/ACCESS.2022.3208650

Provided by King Abdullah University of Science and Technology